Final Project Report

Document information	
Project Title	SWIM security solutions
Project Number	14.02.02
Project Manager	THALES
Deliverable Name	Final Project Report
Deliverable ID	D01
Edition	00.01.00
Template Version	03.00.00
Task contributors	
THALES, DFS, EUROCONTROL, NATMIG, INDRA	

Abstract

The project aimed at defining security solutions for SWIM Technical Infrastructure.
The main outputs of the projects are:

- A finalized SWIM risk assessment, containing the assessment of 17 SWIM services, and a list of valued risks
- A comprehensive list of security requirements, technical, procedural or organizational
- A list of security technologies to implement the most critical security controls
- Security Design recommendations for SWIM implementation
- Recommendations for next projects.

Authoring & Approval

Prepared By - *Authors of the document.*		
Name & Company	Position & Title	Date
[redacted] THALES	[redacted]	06/05/2015

Reviewed By - *Reviewers internal to the project.*		
Name & Company	Position & Title	Date
[redacted]	[redacted]	11/05/2015
		11/05/2015
		11/05/2015
		11/05/2015
		11/05/2015

Reviewed By - *Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organisations.*		
Name & Company	Position & Title	Date

Approved for submission to the SJU By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date

Rejected By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date

Rationale for rejection
None.

Document History

Edition	Date	Status	Author	Justification
00.00.01	06/05/2015	Draft	[redacted]	New Document
00.01.00	28/09/2015	Final		Updated from SJU's comments

Intellectual Property Rights (foreground)

This deliverable consists of SJU foreground.

Acronyms

Acronym	Definition
ADD	Architecture Definition Document
AG	Air/Ground
ANSP	Air Navigation Service provider
ATM	Air Traffic Management
ATS	Air Traffic Services
BCA	Bridge Certificate Authority
CA	Certification Authority
DDOS	Distributed Denial Of Service
DNSEC	Domain Name System Security Extensions
DoS	Denial of Service
EATMA	European ATM Architecture
EC	European Commission
ECRYPT	European Network of Excellence for Cryptology
E-SOC	European Security Operations Centre
EUROCONTROL	European Organization for the safety of air navigation
EU	European Union
GG	Ground/Ground
ICAO	International Civil Aviation Organisation
ICT	Information and Communication Technology
ID	Identifier
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force – main standardization body for Internet
ISO	International Organization for Standardization
ISRM	Information Service Reference Model
IT	Information Technology

Acronym	Definition
MFA	Multilateral Framework Agreement
MSSC	Minimum Set of Security Controls
NIST	National Institute of Standards and Technology
PKI	Public Key Infrastructure
SecRAR	Security Risk Assessment Report
SEMG	SWIM Evolution Management Group
SESAR	Single European Sky ATM Research Programme
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SOC	Security Operations Centre
SSG	SWIM Steering Group
SWIM	System Wide Information Management
TI	Technical Infrastructure
TS	Technical Specification
TAD	Technical Architecture Description
WA	Working Area

1 Project overview

P14.02.02 “SWIM security solutions” was a technical project inside the “SWIM technical architecture” workpackage to define security solutions for SWIM (System Wide Information Management).

ATM Security is a growing concern for all those involved in aviation, including air navigation service providers. The security of the information will have to be managed taking into account the fact that more information will be shared between ATM stakeholders, thus exchanges will be increased and will use the SWIM Technical infrastructure as illustrated in the figure below.

The objective was to provide a framework that allows for a stepwise implementation of the security measures as the threat evolves.

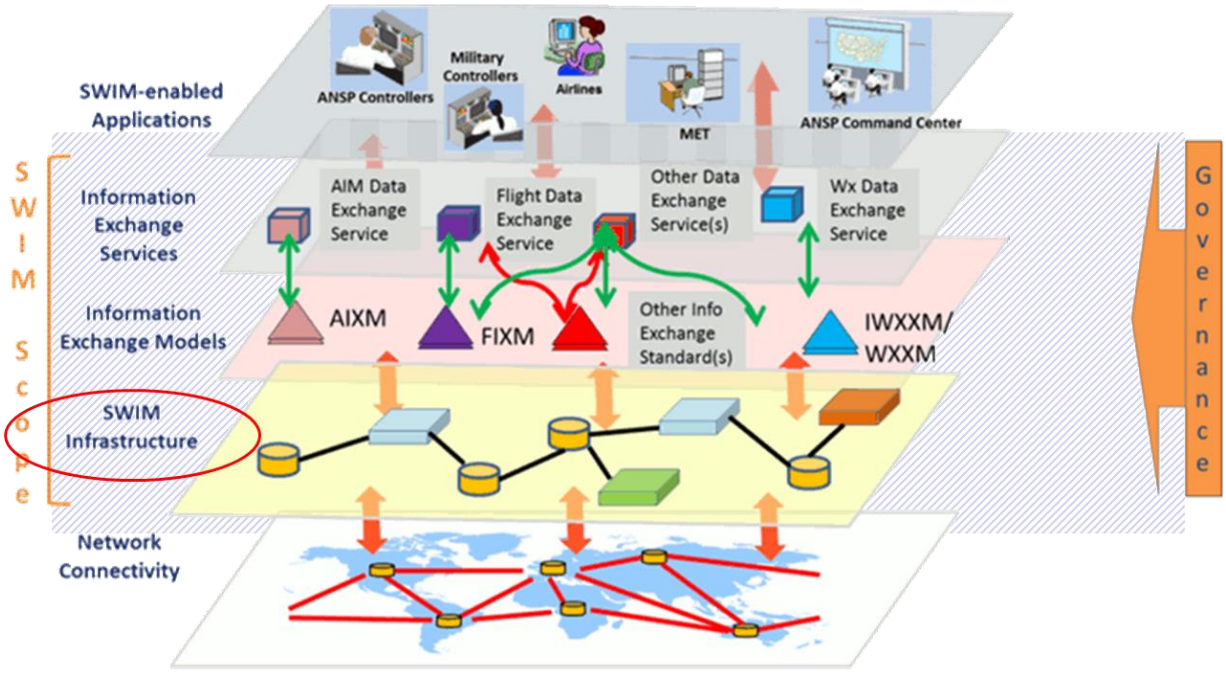

Figure 1: SWIM Technical Infrastructure

SWIM technical infrastructure is shown in the above figure 1.

The technical perimeter was:

- to define and assess ICT (Information and Communication Technology) security solutions for the ground-ground segment of SWIM technical infrastructure (middleware),
- to ensure that the security solutions defined for the ground part of air-ground middleware were consistent with the ones defined for the on-board part.

The project defined a **SWIM security framework**.

- As SESAR ATM Security Requirements were not yet available, SESAR ATM security needs were identified from the SESAR Definition phase. They were taken as a starting point for defining the SWIM Security framework.
- The following list of steps was defined to define security solutions in a top-down approach:
  - identify high-level security requirements
  - perform a security risk assessment in three successive iterations, in order to:
    - cope with the definition of services made in successive iterations, following the delivery of a new set of services in each ISRM. Each ISRM delivery matched the needs of validation exercises.
    - refine the security assessment process for the particular case of SESAR SWIM by learning from previous iterations.

- derive the results of the risk assessment into security requirements as input to the project in charge of producing the SWIM technical infrastructure specification [18], [19], [20], [21].
- define security technologies suitable for SWIM middleware as a complement to the list of possible technologies for SWIM_TI [14]
- define security design solutions, as a complement to the SWIM TI design solutions [15], [16].

The project identified the **SWIM security context and needs**.

- The already existing European and non-European regulations which might be potentially applicable whole or part for SWIM Information security were identified as inputs to defining security requirements.
- Results of previous security studies in the ATM domain or in other domains were identified.
- A first set of High-level security requirements was defined, including a sub-set for interoperability with US SWIM.

The project carried out a **SWIM security risk assessment.**

The result of the SWIM risk assessment is a list of prioritized risks [5].

Security controls were extended to include

- the latest version of the Minimum Set of Security Controls (MSSC)
- the security requirements defined in the SWIM-TI Technical Specification 2.1 and in the SWIM Profiles documents for Step 2 – Iteration 2.1.
- P14.02.02 selected best practices from the widely known security standard NIST SP 800 53 Edition 4 [22].

The project defined the **SWIM security requirements,** it:

- refined the High-level requirements,
- derived requirements from the most critical controls identified by the risk assessment as missing in the definition of SWIM.
- derived requirements from the security controls identified by the second iteration of the risk assessment as missing in the definition of SWIM,
- complemented the MSSC by defining a Statement of Applicability of NIST SP 800 53 standard [22] to SWIM, and derived requirements as inputs to the next iteration of SWIM technical specification, and definition of SWIM organizational and procedural aspects to be defined during deployment.

The project performed an **assessment of available security technologies for SWIM**. The technologies for identity management, authentication, file integrity monitoring and intrusion detection systems.

The project identified **security design solution for SWIM**.

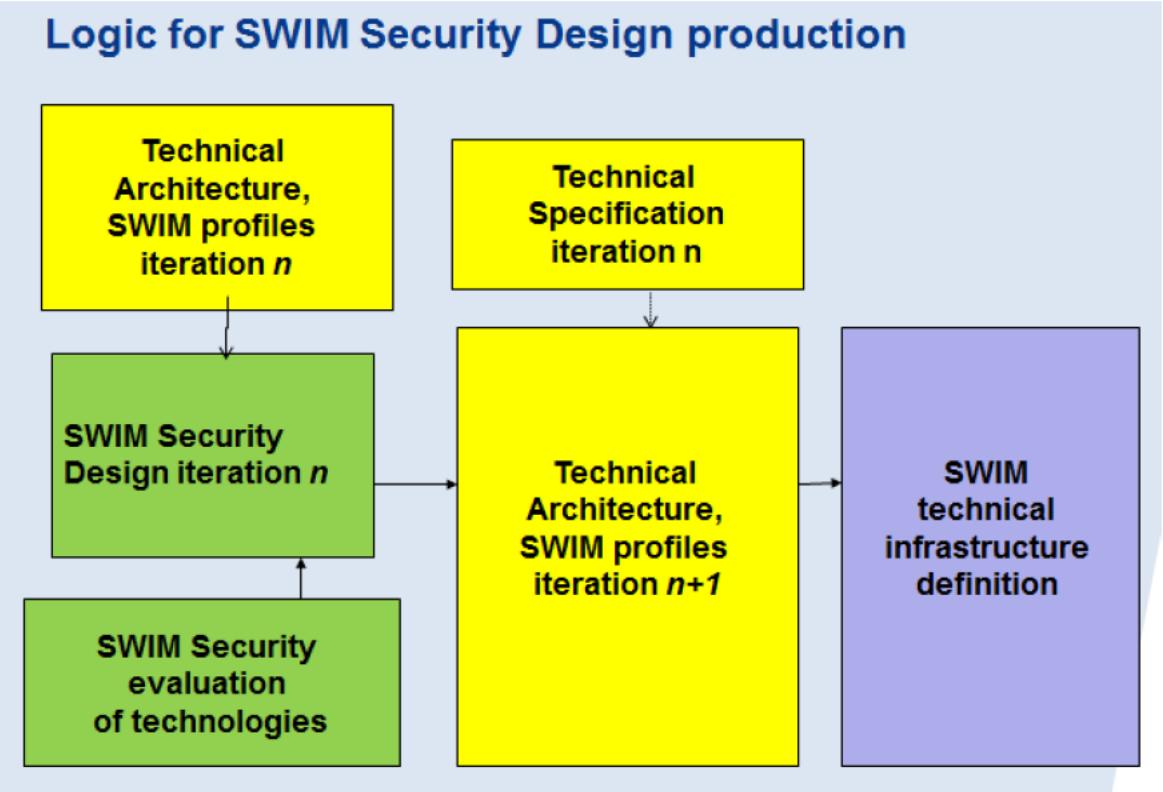

Figure 3: Logic of SWIM security design solutions production

1.1 Project progress and contribution to the Master Plan

The activities addressed by P14.02.02 contributed to the following system Enablers:

Code	Name	Project contribution	Maturity at project start	Maturity at project end
SWIM-SUPT-03a	SWIM Supporting Security Provisions	Assessment of possible technologies, encryption algorithms and design solutions for key management.	V2	V3
SWIM-SUPT-03b	SWIM Supporting Security	Definition of Security requirements, assessment of available technologies and provision of design solutions identity management, authentication, encryption.	V2	V3
GGSWIM-59c	SWIM security in Step3	Definition of security at transport and message level, identity management (local and federated) to provide authentication and authorization. Comparison of risk assessment and types of	V2	V3

Code	Name	Project contribution	Maturity at project start	Maturity at project end
		security controls in ground-ground and air-ground SWIM.		

P14.02.02 contributed to SESAR solution System Wide Information Management.

1.2 Project achievements

A summary of the project achievements is presented below:

- Identification of security context, applicable regulations, and high-level requirements, in particular the ones for interoperability with US SWIM.
- Participation to the definition of the process to develop services for a better integration of security aspects in the service definition.
- A finalized SWIM risk assessment was produced, resulting in a list of risks and dedicated security controls. This analysis includes:
  - some operational inputs from Military, Airspace Users and operational experts, some of them non-SESAR experts.
  - security recommendations coming from the "Terrestrial communication infrastructure - SWIM backbone" [11].
- A comparison of the risk assessments performed for air-ground and ground-ground segments was documented in D26 SWIM Security requirements for iteration 3.0 [6]; the lists of threats and types of security controls were compared, no major discrepancy was discovered. The compatibility of security solutions on-board and on ground is to be established by other SWIM projects, as further work is needed to define architecture solutions.
- A list of Security requirements documented in D26 [6] taking into account the Minimum set of Security Controls [10], but also the NIST SP 800 53 standard [22]. These requirements, which translate best practices relevant for SWIM TI have to be derived either in detailed technical requirements for SWIM TI in the next iteration of the Technical Specification, or in procedural or organizational requirements. The procedures might depend strongly on the implementation choices, so they should be probably defined during SWIM deployment. The organizational requirements should be taken into account during the definition of SWIM governance, as all Stakeholders must be involved.
  The last deliverable D26 [6] provides traceability with High-level requirements, Risk assessment, MSSC, NIST SP 800 53 standard [22], and security requirements from first iterations of the SWIM Technical Specification.
- A list of security technologies suitable for SWIM TI to implement the most critical security controls identified in the risk assessment.
- A list of Security design recommendations was produced.

1.3 Project deliverables

A summary of the project deliverables is presented in the table below:

Del. code	Del.Name	Description

Del. code	Del.Name	Description
D03 [2]	Security context and needs analysis	Security context and needs analysis document pictures out: • The overall SESAR ATM security needs set from the SESAR Definition phase, which is taken as starting point for defining the SWIM Security issues. • The already existing European and non-European regulations which might be potentially applicable whole or part for SWIM. Information security has been already addressed in other domains such as banking, trading, health care, IT communication, and military; thus a number of information security regulations are already defined. Document also gives an insight of the target SWIM Technical Infrastructure which might lead to specific security requirements. A list of existing technologies is also given. Document provides respectively, the assumptions and lessons learned taken as input to develop the SWIM High Level Security Requirements from different points of views: ATM self-protection; security incident management; Civil-military solutions and security criteria for the evaluation of supporting SWIM technologies and services options.
D04 [3]	SWIM security framework - updated	SWIM security framework document presents SESAR ATM security KPA and objectives; ATM Self Protection and Collaborative support. The initial proposed End-to-End SWIM security engineering, which could be composed of a set of phases, was described. Document also provides the SWIM Security Management tools proposed to implement the appropriate measurements in order to eliminate or minimize the impact that security threats and vulnerabilities might have on information and information infrastructure assets.
D19 [4]	Security technologies evaluation - for iteration 2.1	The document consists in a bottom-up approach by evaluating technologies from a security viewpoint. It analyses technologies supporting specific security functions, for instance PKIs, or encryption solutions. It identifies also technology for security features that could be used on the server hosting the SWIM TI middleware. Traceability of each technology with requirements of SWIM technical specification is provided.
D23 [5]	SWIM Security Risk Assessment update for iteration 3.0	17 SWIM services and the information on the SWIM technical infrastructure derived from the SWIM-TI Technical Specification were assessed. A vulnerability assessment was carried out and the result of the assessment is a list of valued risks. In terms of mitigating effects security measures include: • the latest available draft version of the Minimum set of system security controls and • the security requirements defined in the SWIM-TI Technical Specification and in the SWIM Profiles documents, • best practices that were selected from the widely known standard NIST SP 800 53 [22]. The outcomes of this document – together with the proposed additional reviews - permit to build a complementary set of mandatory security requirements mitigating SWIM security risks.
D26 [6]	SWIM security spec-design for iteration 3.0	This document lists all the security requirements identified for SWIM including those for middleware, a few ones related to SWIM infrastructure, and a lot of them related to procedures and organization. These requirements are: • derived from the controls identified as mitigations in SWIM security risk assessment [5], • implementing the minimum set of security controls [19], • or implementing the NIST SP 800 53 [22]/ISO 27002 [39] standard.

Del. code	Del.Name	Description
		The use of standard of security best practices guarantees a consistent coverage of the selected controls for technical, procedural and organizational areas. Non-technical controls are derived in non-technical requirements distinct from technical ones as they should be forwarded to different SESAR projects. Whereas security for purple profile needs further research work, security requirements and design solutions for airborne SWIM were analysed and traceability between both risk assessments is documented in Appendix B of this document.

1.4 Contribution to standardization

P14.02.02 used:

- the draft MSSC [17] produced by SESAR. P14.02.02 made remarks on this document to complement the list of controls with the controls identified during the SWIM risk assessment.
- The NIST standard SP 800 53 [22]. P14.02.02 produced a statement of applicability of NIST to SWIM could be used to perform an update of the MSSC for post SESAR 1 projects.

This work could be used also to enhance the first version of EN 16495 “Air Traffic Management — Information security for organisations supporting civil aviation operations” [24].

1.5 Project conclusions and recommendations

A summary of the project main conclusions and recommendations is presented below.

SWIM risk assessment results and security requirements are being integrated into SWIM definition.

However, the risk assessment should be further reviewed by Stakeholders’ security representatives to validate the work done by P14.02.02.

Then, the SWIM risk assessment produced by P14.02.02 can be used as a starting point for the assessment of a specific SWIM TI implementation.

The recommendations made by the project are of different types, some for the organisational aspects of SWIM security, some for technical security solutions:

1. It is necessary to set up SWIM security governance, with responsibility before and after SWIM TI is put into operation.
   The tasks would first be to ensure:
   - the continuous monitoring and regular assessment of security technologies applied
   - the update of the SWIM risk assessment made by SESAR with additional operational inputs and new design / technological choices,
   - the definition of the SWIM accreditation process to ensure a level of trust for a SWIM service provider/consumer,

   Then, once SWIM TI is in operation the tasks would be:
   - the decision making process and responsibilities for security technology changes,
   - the stakeholder-wide change management,
   - a dynamic risk assessment process, to take into account monitoring data to update the risk assessment. Defining this process could be a subject for a new research project
   - the enforcement of the SWIM accreditation process,
   - the continuous monitoring and assessment of the security technologies applied.
   - the consideration of vulnerabilities in SWIM operational management (i.e. elevation of monitoring means when a security technology is broken).

2. For SWIM security technical solutions:
    - the need to identify the appropriate means to prevent Distributed Denial of Service (DDOSes), which could be a subject for a new research project,
    - the possibility to use Domain Name System Security Extensions (DNSSEC) as a low cost alternative to Bridge Certificate Authority (BCA) /Public Key Infrastructure (PKI), which could be a subject for a new research project.
    - the need to identify common components of SWIM Technical Infrastructure (Registry, Identity Management) that could be certified,
    - the need to ensure that local supervision will be able to cooperate with a European Security Operations Centre (E-SOC),
    - More generally, security engineering principles should be defined for SWIM, which could be a subject for a new research project.

3. For SWIM architecture;
    - SWIM architecture is currently not detailed into software components, it remains functional. Solutions are proposed for each functional block. They are to be considered as recommendations made to an architect to implement security features, in particular for identity management, authentication and log management.
    - The overall recommendation is to ease the integration of security controls by hiding the complexity of the underlying technical functions in order to enable future replacement of a technical product or technology by another one.

2 References

[1] European ATM Master Plan, Edition 2

[2] P 14.02.02-D03 Security context and needs analysis Edition 00.02.00 11 February 2011

[3] P 14.02.02-D04 SWIM security framework – updated Edition 00.01.00 21 October 2011

[4] P 14.02.02-D19 SWIM Security evaluation of technologies Edition 00.01.00.0 27 January 2014

[5] P 14.02.02-D23 SWIM Security Risk Assessment Edition 00.01.01 14 January 2015

[6] P 14.02.02-D26 SWIM Security Requirements for iteration 3.0 Edition 00.01.00 10 April 2015

[7] P 08.03.10-D61 ISRM 1.1 Delivery Report D61 Edition 00.01.00 31 May 2014

[8] P16.06.02-D102, SESAR ATM Security Reference Material - Level 1, Edition 00.05.01 22 December 2014

[9] P16.06.02-D102, SESAR ATM Security Reference Material - Level 2, Edition 00.04.01 20 December 2014

[10] P 16.02.05-D05-006 Minimum Set of Security Controls Edition 00.00.06, 28 February 2014

[11] P 15.02.10-D06 SWIM Backbone Security Management Edition 00.01.00, 8 May 2013

[12]P 09.19-D05 Air-Ground Security Context Definition, Risk Assessment and Security Requirements edition 00.02.01 29 April 2014

[13] P 09.19-D06 SWIM A-G System Architecture, Functional Specification and Technical Requirement Specification edition 00.01.00 27 September 2011

[14]P 14.01.02-D07 Ground/Ground Technology & Service Option Survey - Final Report (Step2), Edition 00.01.00

[15] P 14.01.03-D35 SWIM (GG AG) Architectural Definition for Step 3 - Iteration 3.0 Edition 00.01.01 9 December 2014

[16] P 14.01.03-D36 SWIM Profiles for Step 3 - Iteration 3.0 Edition 00.01.00 9 December 2014

[17]P 14.01.04 D42-002 SWIM-TI Identity Management Technical Specification 3.0 Edition 00.02.00 26 February 2015

[18] P 14.01.04 D42-003 SWIM-TI Run-Time Registry Technical Specification 3.0 Edition 00.02.00 26 February 2015

[19] P 14.01.04 D42-004 SWIM-TI Yellow Profile Technical Specification 3.0 Edition 00.02.00 26 February 2015

[20] P 14.01.04 D42-005 SWIM-TI Blue Profile Technical Specification 3.0 Edition 00.02.00 26 February 2015

[21] P 14.01.04 D42-006 SWIM-TI Purple Profile Technical Specification 3.0 Edition 00.02.00 26 February 2015

[22] NIST Special Publication 800-53 Revision 4 - April 2013

[23] ISO/IEC 27005:2011 - Information technology -- Security techniques -- Information security risk management

[24] EN 16495 Air Traffic Management — Information security for organisations supporting civil aviation operations – Final draft ICS 03.220.50; 35.040 August 2013

-END OF DOCUMENT-